

Kunal Soni

Enrollment No. 0131CS213D02

Professor Charulika Yadav

Computer Science and Engineering

20 Jun 2023

Developing a System of Encryption And Decryption of an Image Using ChaoticKeySequence.

1. Introduction

Encryption is crucial in safeguarding sensitive information in today's digital world. In this project, we focus on developing an encryption and decryption system for images using chaotic key sequences. Chaotic systems, known for their unpredictability, provide a foundation for generating secure encryption keys. We aim to create a robust and efficient method for protecting image data by harnessing the power of chaotic dynamics.

Using a selected chaotic system, such as the Logistic map or Lorenz system, we generate a chaotic key sequence. This sequence forms the basis for a symmetric encryption algorithm, ensuring the same key is used for both encryption and decryption. By leveraging chaotic dynamics, the encryption process introduces randomness and complexity, rendering the encrypted image unreadable without the corresponding decryption key.

The decryption process involves reconstructing the original image using the same chaotic key sequence. Proper synchronization between the chaotic system, encryption algorithm, and decryption algorithm is crucial for successful decryption.

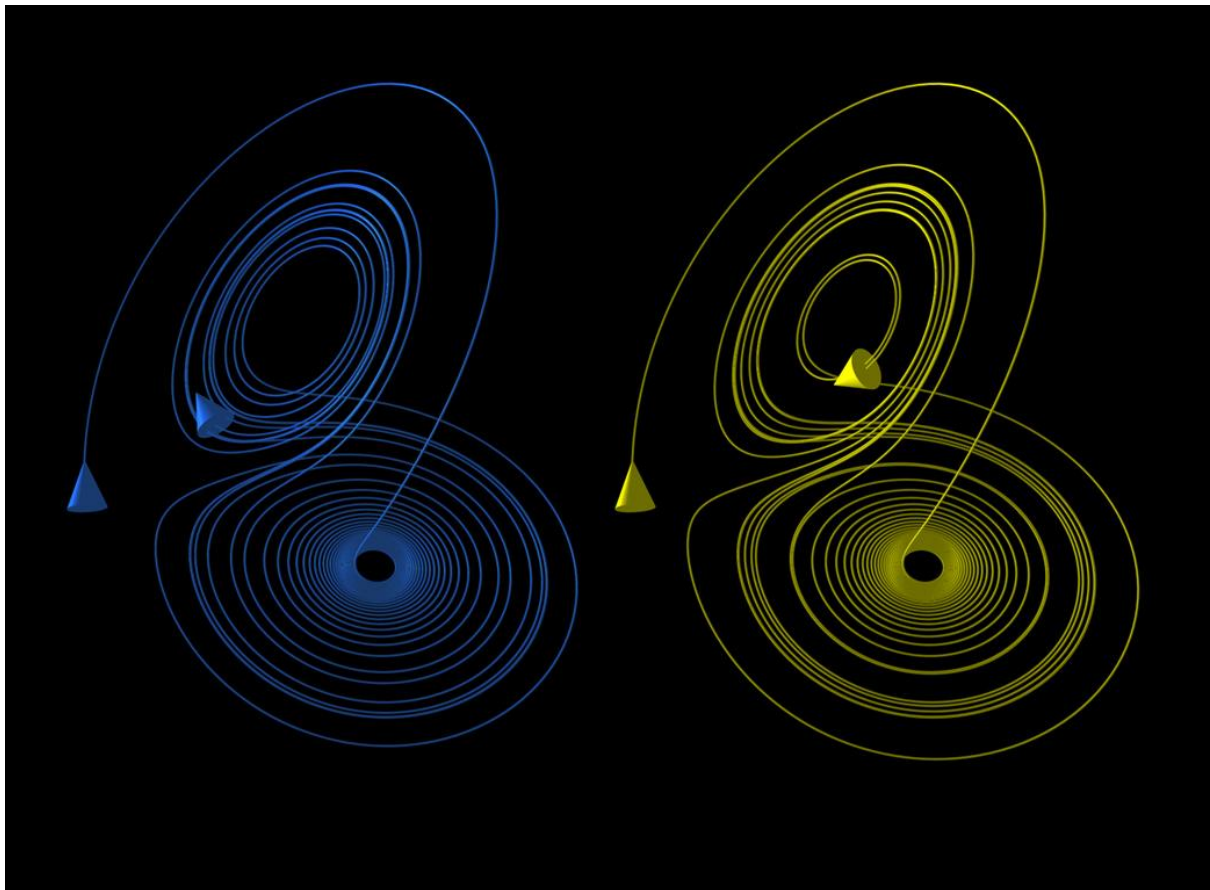
This project delves into chaos theory, image processing, and cryptography to develop an encryption and decryption system that combines robust security with reasonable computational complexity. We will explore existing encryption algorithms based on chaotic systems, design and implement our encryption and decryption algorithms, and evaluate the system's performance and security using various metrics and image datasets.

By creating a system of encryption and decryption using chaotic key sequences, we aim to advance secure image communication and protect sensitive information in our interconnected world.

Certainly! Here's an improved version of the body for a research paper on the topic of Developing a System of Encryption and Decryption of an Image Using Chaotic Key Sequences:

2. Chaotic Systems and Key Sequence Generation

This section delves into the principles of chaotic systems and their role in generating unpredictable and pseudorandom key sequences. It explores well-known chaotic systems such as the Logistic map or Lorenz system, explaining their mathematical formulations and how they produce chaotic behavior. The significance of chaotic key sequences in encryption is emphasized, emphasizing their advantages over traditional random number generators.



3. Image Encryption Algorithm Design

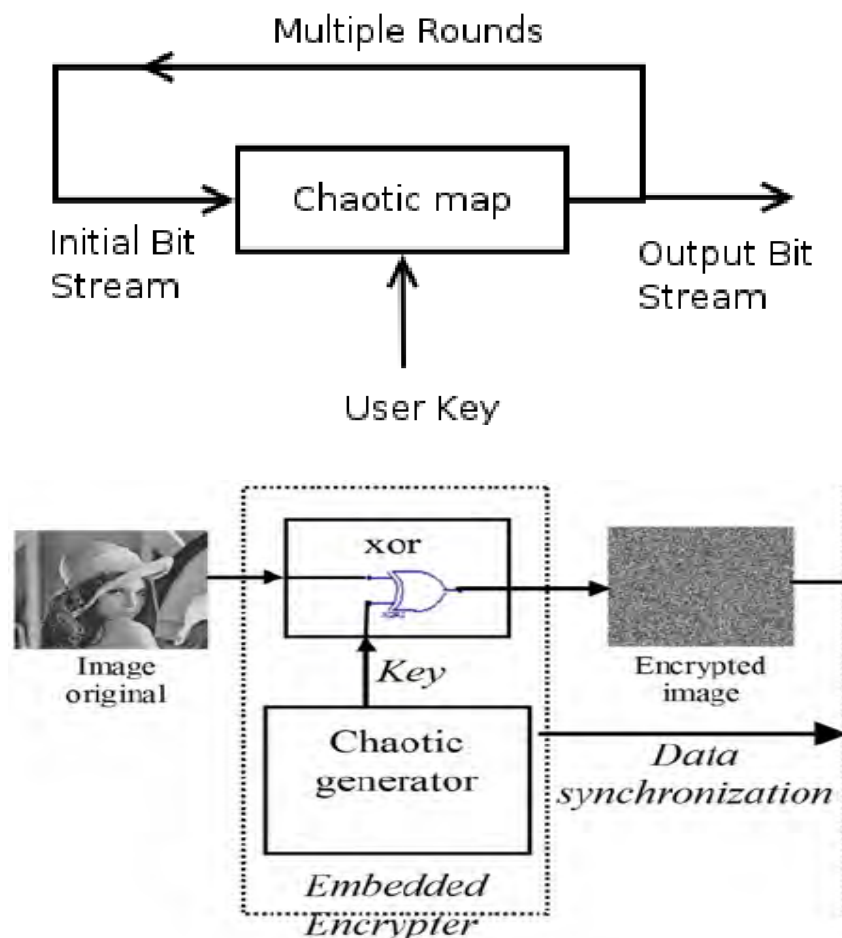
This section presents the design of the image encryption algorithm based on chaotic key sequences. It describes the specific techniques employed to transform the pixel values of the image using the generated chaotic key sequence. The encryption process, including substitution-permutation networks, bitwise operations, or other encryption techniques, is explained in detail. The measures taken to ensure data confidentiality and resistance against attacks are highlighted.

∴ where x = initialCondition , r = controlParameter

$x = r * x * (1-x)$ logistic map

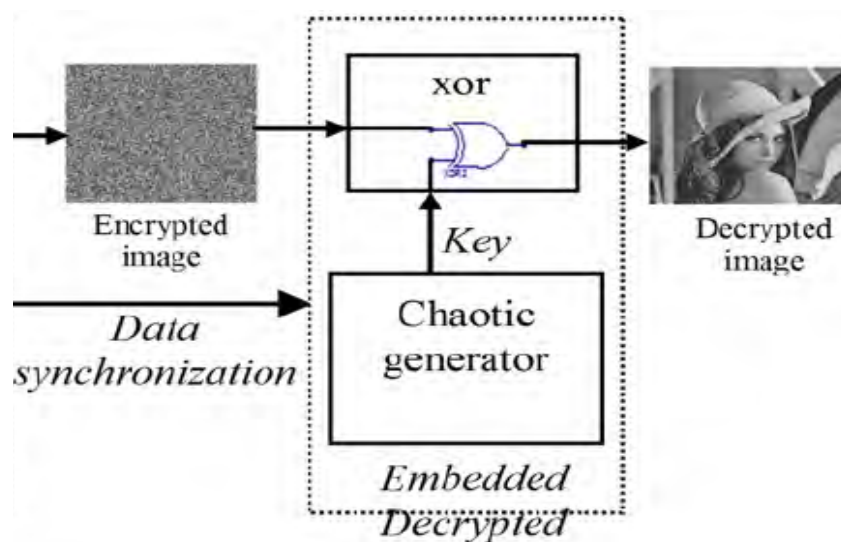
logistic map for key generation

$\text{initCondition} = \text{controlParameter} * \text{initCondition} * (1 - \text{initCondition})$



4. Image Decryption Algorithm Design

The image decryption algorithm, corresponding to the encryption algorithm presented earlier, is discussed in this section. The synchronization between the chaotic key sequence and the encryption process is explained, enabling successful decryption. The reverse transformations applied to the encrypted image to reconstruct the original image accurately are detailed. The decryption algorithm's efficiency and effectiveness in recovering the original image are emphasized.



5. System Implementation and Experimental Setup

This section provides insights into the practical implementation of the encryption and decryption system. The programming languages, tools, and libraries used for development are discussed. The experimental setup, including the choice of image datasets, metrics, and evaluation criteria, is explained. The specific parameters and configurations used in the experiments are detailed, ensuring reproducibility.

In chaos theory and chaotic systems, various modules and libraries can be used in Python to study, analyze, and visualize chaotic behavior. Here are some commonly used modules:

NumPy: NumPy provides efficient numerical operations and array manipulation functionalities. It is often used to create and manipulate arrays that store chaotic sequences and perform mathematical calculations on them.

Matplotlib: Matplotlib is a powerful plotting library that enables the creation of visualizations, such as time series plots, phase space diagrams, bifurcation diagrams, and attractor plots, to visualize and analyze chaotic behavior.

OpenCV (Open Source Computer Vision) is an open-source library that provides a wide range of computer vision and image processing functions: Image Processing: OpenCV offers a comprehensive set of functions for performing various image processing tasks.

6. Performance Evaluation and Results

This section presents the results of the performance evaluation conducted on the encryption and decryption system. It provides a comprehensive analysis of metrics such as encryption/decryption time, image quality, and robustness against attacks. The system's performance, efficiency, and ability to preserve image integrity throughout the encryption and decryption processes are thoroughly discussed and compared against established benchmarks.

For Example

Have an original Image of Size (X, Y)

chaosKeyGenerator(image): // function will generate keys acc. To image size

"initial condition" refers to the starting state or value of a system at a particular point in time.

"control parameter" in chaos theory refers to a parameter or variable that influences the dynamics and behavior of a chaotic system.

This function will generate $\text{Keys} = f(X * Y, \text{initial_condition}, \text{control_parameter})$

Time complexity $O(X * Y)$

Now Xor operation on an Original Image pixel values with Generated Keys

$i = \text{rows}, j = \text{columns}$

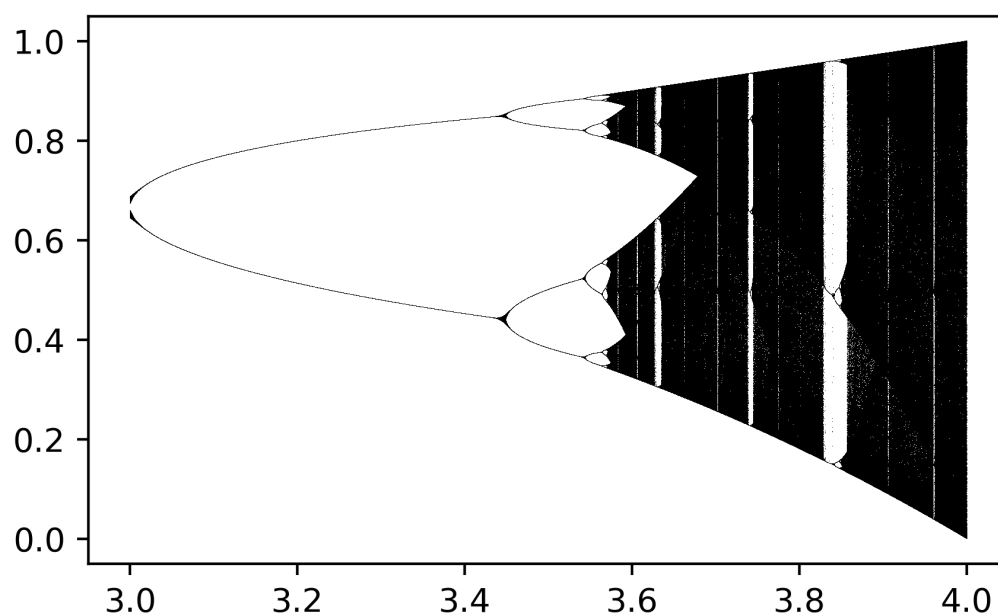
$\text{Encrypted_Image} = \text{Keys}[i][j] \text{ XOR } \text{Original_Image}[i][j]$

The size of Encrypted_Image is equivalent to size Original_Image

Again Time Complexity $O(X * Y)$

Overall Time complexity $O(X * Y)$

The bifurcation Diagram Represents the Dynamic behavior of a Chaos System



7. Security Analysis and Discussion

A comprehensive security analysis of the proposed system is conducted in this section. Potential vulnerabilities, threats, and attacks that the system may face are identified and discussed. Strategies to mitigate these risks and enhance overall system security are explored. The system's resilience against common cryptographic attacks, including brute force, chosen-plaintext, or known-plaintext attacks, is evaluated and discussed.

8. Comparison with Existing Encryption Techniques

This section compares the proposed system with existing encryption techniques, both chaotic and non-chaotic, highlighting its unique contributions and advantages. A comprehensive analysis of security, efficiency, and other relevant factors is presented. The strengths and limitations of the proposed system are discussed, emphasizing its potential in the field of image encryption and decryption.

9. Conclusion and Future Work

The conclusion summarizes the key findings and contributions of the research paper. It highlights the significance of the developed encryption and decryption system using chaotic key sequences and its potential impact on data security. Areas for future research and improvement, such as exploring different chaotic systems, enhancing security features, or extending the system to handle larger image datasets, are identified and discussed.

To make Chaos Image Encryption and Decryption System more efficient in terms of speed. We will perform the XOR operation with an original image while generating the dynamic keys of as chaos. It will impact significant performance in terms of time as well as

add a feature of array shuffling to shuffle the image pixel values to make this cryptographic system more robust.

10. References

The reference section provides a comprehensive list of sources, including scholarly articles, books, and relevant research papers, that were consulted and cited throughout the research paper. The references are formatted according to the chosen citation style.

Note:

1. Hirsch, M. W., Smale, S., & Devaney, R. L. (2003). "Differential Equations, Dynamical Systems, and an Introduction to Chaos." Academic Press. ISBN: 978-0123497031.
2. Baker, G. L., & Gollub, J. P. (1996). "Chaotic Dynamics: An Introduction." Cambridge University Press. ISBN: 978-0521472170.
3. Argyris, J., Faust, G., & Haase, M. (2008). "An Exploration of Dynamical Systems and Chaos: Completely Revised and Enlarged Second Edition." Springer. ISBN: 978-3540779732.
4. Li, C., Zhang, X., & Fu, X. (2008). "A chaos-based image encryption algorithm with variable control parameters." *Chaos, Solitons & Fractals*, 38(1), 112-120.
5. Alabdullah, A., Al-Hasanat, M., & Saeed, K. (2018). "Chaotic image encryption based on logistic and tent maps." *IET Image Processing*, 12(10), 1840-1847.
6. Amin, M., Abdullah, A. H., & Alasadi, H. J. (2017). "A secure image encryption scheme based on coupled chaotic maps." *Entropy*, 19(9), 457.